U.S. Department of Justice

United States Attorney
Eastern District of New York

eAB:SSS/GMM
F.#2016R02185

271 Cadman Plaza East
Brooklyn, New York 11201

September 18, 2019

By Hand and ECF

Honorable Kiyo A. Matsumoto
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: United States v. Ingrid Innes
Criminal Docket No. 18-134 (S-2)(KAM)

Dear Judge Matsumoto:

The government respectfully submits this letter in further support of its motion requesting that the Court find that a document created by above-referenced defendant Ingrid Innes (the "Document") is not protected by the attorney-client privilege ("Gov't Mot.") and in reply to the defendant's response filed on September 13, 2019.

I. The Defendant Did Not Have a Reasonable Expectation that the Document Saved on Her Company-Owned Tablet Computer Would Remain Confidential

The defendant argues that she had a reasonable expectation that the Document would remain confidential because, among other things, she created it while she was "out of the office on vacation." Def.'s Response in Opp., Dkt. 73, at 4. The defendant, however, was not merely "on vacation." She had been suspended from work and told to minimize her use of company equipment. Specifically, on October 4, 2016, John Wight, the President and Chief Executive Officer of BF&M Limited, the parent company of the Insurance Corporation of Barbados Limited ("ICBL"), confronted the defendant about bribing her co-defendant Donville Inniss, a government official in Barbados. See Ex. B to Gov't Mot., at 1. The following day, Wight told the defendant that she was immediately suspended from work, with pay, pending an "independent investigation" into what she had done. Id. Wight told the defendant that it was "good" that she was planning to go on vacation the following day because "from the perspective of anyone outside the board of directors, her absence from the office for the next 2 plus weeks would be seen as nothing other than vacation." Id. In addition, Wight told the defendant that she would receive a suspension letter on her "personal e-mail address" – not her work e-mail address. Id. Wight also instructed the defendant that she was "entitled to read ICBL e-mail, but not to respond to anything" and that "[i]f there was an e-mail that required action on behalf of the company," the defendant "was to advise [Wight] accordingly and [he] would act upon it." Id.

Four days later, on October 9, 2016, the defendant used her work tablet computer – which ICBL's Code of Conduct made clear had been provided for "business use" and "must not be used . . . in support of any . . . outside daily activity" – to create and store the Document. Ex. C to Gov't Mot., at 1; Ex. F to Gov't Mot., ¶¶ 1.11.1, 1.11.3.

As a suspended ICBL employee who was under investigation and had been instructed only to read – but not respond to – company e-mails, it was unreasonable for the defendant to believe that she was even allowed to use the tablet for any purpose other than reading work-related e-mails, much less reasonably believe that, despite ICBL's policy banning personal use of company computers, she was permitted to create and store the Document on her company-owned tablet computer, and that it would remain confidential.[1]

A. ICBL's Code of Conduct Banned Personal Use of the Company-Owned Tablet Computer

The defendant also argues that ICBL did not have a policy expressly prohibiting employees from using company equipment for personal matters. Def.'s Response in Opp., at 5. However, the plain language of the ICBL Code of Conduct states that company-issued computer equipment is "for business use" and "must not be used . . . in support of any . . . outside daily activity." Ex. F to Gov't Mot., ¶¶ 1.11.1, 1.11.3. The defendant does not, and cannot, explain why working on a personal legal matter is not an "outside daily activity" that is prohibited under the Code. Because ICBL's Code of Conduct bans all personal use of company computers, the defendant's reliance on United States v. Hatfield, No. 06-CR-0550 (JS), 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009), is misplaced. In Hatfield, the company's policy contained a general "expect[ation]" that employees would use company equipment solely for business purposes, but strictly prohibited only a few specific activities, which did not include working on personal legal matters. Id. at *9. Here, by contrast, ICBL's policy bans use of computer computers for "any . . . outside daily activity." Ex. F to Gov't Mot., ¶ 1.11.3 (emphasis added).

B. A Third Party Had Access to the Company-Owned Tablet Computer

The defendant also contends that the government has conceded that ICBL did not regularly grant third parties the right to access ICBL's computers or e-mails. Def.'s Response in Opp., at 6. It is also clear, however, that ICBL – itself a third party to the defendant and her attorney – could access the defendant's tablet by requiring her to return it, as ICBL in fact did

[1] On October 23, 2016, Wight e-mailed the defendant at her personal e-mail address and explained that her "access to the [ICBL] system [would] be removed tomorrow morning, and that during the suspended period, the company issued laptop and phone [would need to] be returned to the company." Ex. D to Gov't Mot., at 5. The defendant objected and, on October 25, 2016, Wight granted her request to retain access to the ICBL computer system, provided that KPMG would "secure and image" her "Company issued laptop and mobile device," which would then be returned to her. Id. at 2-4. This e-mail exchange shows that the defendant did not ask Wight between October 5, 2016, and October 23, 2016 – the period in which she created the Document – for permission to use company-issued equipment for any purpose other than reading work-related e-mails.

here, and that the ICBL Code of Conduct made clear to the defendant and other employees that the company "reserve[d] the right to monitor or review all data and information contained on an employee's Company-issued computer or electronic device." Ex. F to Gov't Mot., ¶ 1.11.4. As in Hatfield, "this factor tips against a finding of privilege." Id. at *9 (noting that the company for which the defendant worked "unquestionably had a right to access [the defendant's work] computer" (emphasis in original)).

II. The Defendant's Careless Disclosure of the Document to KPMG Constituted Waiver, Even if the Document Were Privileged

The defendant also argues that when she turned over the company-issued tablet to KPMG to be searched, she had "simply forgot[ten]" that she had saved the Document on it two-and-a-half weeks earlier. Def.'s Response in Opp. at 3. As an initial matter, the government is limited in its ability to respond properly to the defendant's assertion because her affidavit was filed under seal "to preserve her attorney client privilege" and not provided to the government. Def.'s Response in Opp. at 1, n.1. It is unclear, however, how the defendant's explanation for why she "forgot" to delete the Document would be a statement protected by the attorney-client privilege. The government requests that the Court order the defendant to unseal all portions of her declaration that are not protected by the attorney-client privilege.

The defendant argues that she did not waive the privilege by disclosing the Document to KPMG because she took "reasonable precautions" to prevent inadvertent disclosure by saving the Document on the local hard drive of her company-issued tablet and not on the ICBL server. Def.'s Response in Opp. at 7. Under the circumstances of the defendant's suspension and ICBL's investigation into the defendant, that single precaution was not reasonable. It was careless and not indicative of any reasonable intention to maintain confidentiality over the Document. For example, the defendant did not label the document "attorney-client privileged" or "confidential." Nor did the defendant password-protect the Document or save it in a unique folder indicating that it was privileged, confidential, or even merely personal. Instead, she saved it in the generic "Documents" folder on the tablet computer. See Ex. C to Gov't Mot., at 1. And most importantly, the defendant did not delete the Document after apparently e-mailing it to her attorney. See Curto v. Med. World Commc'ns, Inc., No. 03-CV-6327 (DRH) (MLO), 2006 WL 1318387, at *1, 3 (E.D.N.Y. May 15, 2006) (finding that the plaintiff took reasonable precautions to prevent inadvertent disclosure of privileged materials where, after "she was instructed to return" her work-issued laptop to her company, she "deleted all personal files and written communications to counsel," which were subsequently restored by a foreign consultant). This is not a situation where the defendant had created the Document years, or even months, prior to turning the tablet computer over to KPMG. Instead, the defendant created the Document – which is a chronology of events that was obviously relevant to KPMG's investigation of the defendant – a mere 17 days before she turned over the tablet to KPMG, so it could search for documents relevant to its investigation. Indeed, on October 26, 2016, the defendant informed Wight that after she dropped off her work laptops and cell phones to KPMG, she "realised" that she also had an "IPad." Ex. E to Gov't Mot., at 1. The defendant further noted that "[e]mails are not on the IPad," which shows that she thought about what types of materials were saved on the company-owned tablet computer that contained the Document. Id. Finally, even if the defendant had forgotten about the Document in particular, there is no

evidence that the defendant told KPMG that there were personal documents on her company tablet computer which, had she done so, may have notified KPMG of the possibility that the tablet contained potentially privileged information. In short, the defendant took zero precautionary steps to preserve the confidentiality of the Document, other than saving it in the "Documents" folder on her work tablet.

The defendant also argues that she took reasonable precautions because, like the plaintiff in Curto, she attached the Document to an e-mail that she sent through her personal e-mail address. Def.'s Response in Opp. at 7. However, that issue is not before the Court. The Document is not an e-mail that the defendant sent through her personal e-mail account that was later forensically recovered from the tablet computer, like the recovered e-mails in Curto. 2006 WL 1318387, at *1 ("The [forensic] consultant was able to restore portions of the computer files and e-mails that had been deleted by Plaintiff." (emphasis added)). Instead, KPMG found the Document in the "Documents" folder of the tablet. See Ex. C to Gov't Mot., at 1. In Curto, as here, the plaintiff also claimed privilege over certain computer files that she had saved on her company laptop. Curto, 2006 WL 1318387, at *2. The court in Curto stated that the plaintiff had taken reasonable precautions to prevent inadvertent disclosure of the computer files because she "attempted to delete" those files from the laptop before she returned it to her company, which were later recovered through a forensic analysis. Id. at *3. By contrast, the defendant here took no such precaution.

For the foregoing reasons, the government's request that this Court find that the Document is not protected by the attorney-client privilege should be granted, and the government should be permitted to use the Document in its prosecution of the defendant and produce it to the defendant Donville Inniss in discovery.

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

By: /s/
Sylvia Shweder
Assistant U.S. Attorney
(718) 254-6092

ROBERT A. ZINK
Chief, Fraud Section
U.S. Department of Justice

By: /s/
Gerald M. Moody, Jr.
Trial Attorney
U.S. Department of Justice
(202) 616-4988

cc: Ronald G. DeWaard, Esq., counsel to Ingrid Innes, and all other counsel of record